Kyle McLean, Esq. (SBN #330580)
Email: kmclean@sirillp.com
Mason Barney, Esq.
Email: mbarney@sirillp.com
Tyler Bean, Esq.
Email: tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CHERRI THOMAS, individually and on behalf of themselves and all others similarly situated, Plaintiff, v. **CEREBRAL INC.**, a Delaware corporation, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Cherri Thomas ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Cerebral Inc. ("Cerebral" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Cerebral, a healthcare corporation headquartered in California, for its unauthorized transmission and disclosure of Plaintiff's and other similarly situated Cerebral patients' highly sensitive and confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to herein as "Private Information") to Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") and/or TikTok Inc. ("TikTok") via a tracking pixel (the "Tracking Pixel" or "Pixel") installed on Defendant's website, www.cerebral.com (the "Website"), which Defendant owns and controls.

2. Defendant "offers long-term online care and medication management for a wide range of mental health conditions."[1]

3. In order to provide medical treatment and care, Defendant collects and stores its patients Private Information and medical records. In doing so, Defendant must comply with statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that Private Information from disclosure and ensure that it remains private and confidential.

4. Plaintiff and Class Members are similarly situated individuals who are seeking or have sought medical services and/or treatment from Defendant. Defendant advertises its online services on its Website and elsewhere to assist patients with their medical care.

5. Based on its solicitations that patients use its online services, Plaintiff used Defendant's Website to research particular medical concerns and treatments, fill out forms and questionnaires, and perform other tasks related to her particular medical concerns.

[1] *See* https://cerebral.com/faqs#General_questions-How_does_Cerebral_work_ (last visited on April 23, 2023).

6. Defendant's own Privacy Policies unequivocally state that Defendant will not share Plaintiff's and Class Members' Private Information for marketing purposes unless patients provide written permission.[2] Thus, Defendant is duty bound to maintain the confidentiality of its patients' medical records and information and is further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

7. However, based on the following notice email sent to its patients, as well as a report Defendant submitted to the United States Department of Health and Human Services (collectively, the "Notice"), Defendant admits to the use of the Pixel on its Website. Through this unauthorized use of the Pixel, Defendant unlawfully intercepted and transmitted Plaintiff's and Class Members' Private Information, including their names, phone numbers, email addresses, dates of birth, IP addresses, client ID numbers, and demographic and other information:

> **What Happened?**
>
> Like others in many industries, including health systems, traditional brick and mortar providers, and other telehealth companies, Cerebral has used what are called "pixels" and similar common technologies ("Tracking Technologies"), such as those made available by Google, Meta (Facebook), TikTok, and other third parties ("Third Party Platforms"), on Cerebral's Platforms. Cerebral has used Tracking Technologies since we began operations on October 12, 2019. Cerebral recently initiated a review of its use of Tracking Technologies and data sharing practices involving Subcontractors. On January 3, 2023, Cerebral determined that it had disclosed certain information that may be regulated as protected health information ("PHI") under HIPAA to certain Third Party Platforms and some Subcontractors without having obtained HIPAA-required assurances.

[2] *See* https://cerebral.com/privacy-policy (last visited on April 23, 2023).

What Information Was Involved?

The information disclosed varied depending on what actions you took on Cerebral's Platforms, the nature of the services provided by the Subcontractors, the configuration of Tracking Technologies when you used our services, the data capture configurations of the Third-Party Platforms, how you configured your device and browser, and other factors.

- If you created a Cerebral account, the information disclosed may have included your name, phone number, email address, date of birth, IP address, Cerebral client ID number, and other demographic or information.

- If, in addition to creating a Cerebral account, you also completed any portion of Cerebral's online mental health self-assessment, the information disclosed may also have included your selected service, assessment responses, and certain associated health information.

- If, in addition to creating a Cerebral account and completing Cerebral's online mental health self-assessment, you also purchased a subscription plan from Cerebral, the information disclosed may also have included subscription plan type, appointment dates and other booking information, treatment, and other clinical information, health insurance/ pharmacy benefit information (for example, plan name and group/ member numbers), and insurance co-pay amount.

8. Parsing out Defendant's Notice, it has admitted that its Website contained (and may still contain) a Tracking Pixel that secretly enabled the

unauthorized transmission and disclosure of Plaintiff's and Class Members' Private Information to third parties such as Facebook, Google, TikTok, and others.

9. The Private Information disclosed is valuable to internet marketing companies such as Facebook, Google, and TikTok as they receive, view, analyze, and aggregate such Information to build consumer profiles to assist advertisers in targeting desired demographics.

10. Accordingly, the purpose of this lawsuit is to protect Plaintiff's and Class Members' right to protect their Private Information from unauthorized disclosure and use, to choose who receives it and how it is used, and to seek remedies for the harms caused by Defendant's intentional, reckless, or negligent disclosure to unauthorized third parties.

II. JURISDICTION & VENUE

11. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Cerebral. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges violations of the ECPA (28 U.S.C. § 2511, *et seq*., and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*.).

13. This Court has personal jurisdiction over Cerebral because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of

Plaintiff's and Class Members' Private Information; Defendant's principal place of business is located in this District; Defendant collected and redistributed Class Members' Private Information in this District; and Defendant caused harm to Class Members residing in this District.

III. PARTIES

Plaintiff Cherri Thomas

15. Plaintiff Thomas, is, and at all times mentioned herein was, an individual citizen of the State of Arizona residing in the City of Mesa in Maricopa County.

16. Plaintiff Thomas began receiving healthcare services from Defendant in or around 2020 and accessed those services via Defendant's Website. While using Defendant's Website, Plaintiff communicated sensitive (and what she presumed to be confidential) personal and medical information to Defendant.

17. Plaintiff Thomas used Defendant's Website to communicate and research particular medical concerns, fill out forms and questionnaires, and perform other tasks related to her specific medical inquiries.

18. In the course of using Defendant's services, Plaintiff provided her name, phone number, email address, date of birth, and other PII. As a result of the Pixel Defendant installed on its Website, Plaintiff's PII was intercepted, viewed, analyzed, and used by third parties without Plaintiff's knowledge or authorization.

19. Plaintiff also answered Cerebral's online mental health assessment questions and communicated information regarding her particular health condition and concerns, as well as other PHI, to Cerebral through the Website. As a result of the Tracking Pixel Defendant installed on its Website, this PHI was intercepted, viewed, analyzed, and used by unauthorized third parties.

20. As Defendant's patient, Plaintiff Thomas reasonably expected that her online communications with Defendant were solely between herself and Defendant,

and that such communications would not be transmitted or intercepted by a third party. Plaintiff Thomas also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's representations via its Privacy Policies, Plaintiff Thomas would not have disclosed her Private Information to Defendant.

21. During her time as a patient of Defendant, Plaintiff Thomas never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, Google, TikTok, and others, to access or interpret such Information.

22. Notwithstanding, through the Pixel and similar tracking technologies Defendant admits to have embedded on its Website, Defendant transmitted Plaintiff Thomas's Private Information to third parties, including Facebook, Google, TikTok, and others, who then viewed, processed, analyzed, and assimilated such Private Information into data sets used to target Plaintiff with advertising.[3]

23. Plaintiff thus brings this complaint to address this unauthorized transmission and disclosure of her and Class Members' confidential Private Information to Facebook, Google, TikTok, and others via the Tracking Pixel installed on Defendant's Website.

Defendant Cerebral Inc.

[3] Facebook, Google, TikTok, and others offer code to website and mobile application operators, like Defendant, to integrate into their platforms. When a user accesses a platform hosting the Pixel, the Pixel's software script surreptitiously directs the user's browser to send a separate message to a third party's servers during their interaction with the webpage. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by the code concurrently with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code, and the Pixel embedded code.

24. Defendant Cerebral Inc. is a mental health telemedicine company incorporated in the State of Delaware, with its principal place of business and headquarters located at 340 S. Lemon Ave., #9892, Walnut, California, 91789.

IV. FACTUAL ALLEGATIONS

A. The Pixel

25. A "pixel" is a piece of code that "tracks the people and [the] type of actions they take."[4] Pixels are routinely used to target specific consumers by utilizing the data gathered through pixels (and other tracking technologies) to build profiles for the purposes of retargeting and future marketing. The Tracking Pixel embedded on Defendant's Website did just that, such that when a visitor interacted with the Website, two signals were sent in tandem: one to the intended recipient (Defendant), and another to the unauthorized recipient (Facebook, Google, TikTok, and others).

26. Accordingly, when an individual visits Defendant's Website and communicates Private Information to Defendant, the Pixel allows unauthorized parties to listen in to such communications in real time, *i.e.*, they receive the communication as it is communicated to Defendant.

27. Defendant itself acknowledges that the aggregate information captured by the Pixel and disclosed to unauthorized parties includes both PII and PHI. The recipients of this data are able to associate information communicated across multiple visits to the Website by capturing persistent identifiers like IP addresses, browser fingerprints, and device IDs.

28. Facebook, Google, TikTok, and others also use "cookies"[5] installed on Plaintiff's and Class Members' browsers to associate Private Information with

[4] FACEBOOK RETARGETING, https://facebook.com/business/goals/retargeting (last visited on April 23, 2023).

[5] "Cookies" are a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from

particular individuals. For example, with respect to Facebook, the persistent Pixel on Defendant's Website causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other Private Information that is sent to Facebook.

29. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to existing patients. In other words, Defendant implemented the Pixel to bolster its profits.

30. Defendant also regularly encouraged Plaintiff and Class Members to use its digital tools, including its Website, to receive healthcare services. In doing so, Defendant also directed Plaintiff and Class Members to its Privacy Policies, which preclude the transmission or disclosure of Private Information to unauthorized third parties such as Facebook, Google, and TikTok.

31. However, in violation of these Privacy Policies, the Pixel (operating as designed) allowed the Private Information that Plaintiff and Class Members communicated to Defendant to be unlawfully disclosed to third parties.

32. At all times that Plaintiff and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through Defendant's Website, including that it would remain secure and protected and only utilized for necessary purposes. Plaintiff's and Class Members' expectations were entirely reasonable because (1) they are patients; and (2) Defendant is a healthcare provider which is required by common and statutory law to protect its patients' Private Information. Moreover, Plaintiff and Class Members relied on Defendant's Privacy Policies, which do not permit the

---

client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.

transmission or disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties.

33. Defendant further made express and implied promises to protect Plaintiff's and Class Members' Private Information and maintain the privacy and confidentiality of communications that they exchange with Defendant. Instead, Defendant chose to exchange the Private Information to optimize the delivery of its ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Website, and decrease advertising and marketing costs.

34. Cerebral owed common law, contractual, statutory, and regulatory duties to keep Plaintiff's and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that Information from unauthorized disclosure.

35. However, as set forth more fully below, Defendant failed in its obligations and promises by utilizing the Tracking Pixel on its Website knowing that such technology would transmit and disclose Plaintiff's and Class Members' Private Information to unauthorized third parties.

36. The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or to insurance companies utilizing the information to set insurance rates.

37. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure Defendant's Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users'

information; (iii) failing to obtain the consent from Plaintiff and Class Members before disclosing their Private Information to Facebook, Google, TikTok, or others; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' Private Information through Tracking Pixels; and (v) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

38. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) loss of control over their Private Information, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk of exposure and unauthorized use of their Private Information by marketing companies.

39. Defendant also deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented technology (*i.e.*, the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

B. Cerebral's Privacy Policies and Promises

40. Defendant's Privacy Policies unequivocally state Defendant will not share Plaintiff's and Class Members' Private Information for marketing purposes unless patients provide written permission.

41. Plaintiff and Class Members have not provided Defendant with written permission to share their Private Information for marketing purposes.

42. Despite Defendant's acknowledgment that it would not share Plaintiff's and Class Members' Private Information, Defendant, in fact, did share Plaintiff's and Class Members' Private Information via the Pixel.

43. Specifically, Defendant transmitted and/or disclosed Plaintiff's and Class Members' Private Information to third parties, like Facebook, Google, and TikTok, without Plaintiff's and Class Members' consent or written permission.

44. In doing so, Defendant intended to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients.

45. In simple terms, Defendant violated its own Privacy Policies – *i.e.*, the Privacy Policies that Plaintiff and Class Members relied upon – in order to bolster its profits. Such violations of its own Privacy Policies were also in violation of HIPAA.

C. Cerebral Violated HIPAA Standards

46. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[6]

47. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

48. In its guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not

[6] *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

> necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[7]

49. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or his protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.[8]

50. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[9]

---

[7] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited on April 23, 2023).

[8] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited on April 23, 2023).

[9] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited on April 23, 2023).

51. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

52. In other words, HHS has expressly stated that the Pixel violates HIPAA Rules, meaning that there is no question that by implementing the Pixel, Defendant violated HIPAA.

D. Cerebral Failed to Comply with Industry Standards

53. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

54. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting privacy of patient data and communications.

55. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy).

56. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data

> that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted. 176. AMA Code of Medical Ethics Opinion 3.3.2 provides: Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…(c) release patient information only in keeping ethics guidelines for confidentiality.

E. IP Addresses are Personally Identifiable Information

57. On information and belief, through the use of the Pixel on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook, Google, TikTok and/or other third parties with intercepting Plaintiff's and Class Members' computer IP addresses.

58. An IP address is a number that identifies the address of a device connected to the Internet.

59. IP addresses are used to identify and route communications on the Internet.

60. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

61. Facebook tracks every IP address ever associated with a Facebook user. Google also tracks IP addresses associated with Internet users.

62. Facebook, Google, and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

63. Under HIPAA, an IP address is considered personally identifiable information.[10] Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

F. Cerebral was Enriched and Benefitted from the Use of the Pixel

56. The sole purpose of the use of the Pixel on the Website was to increase marketing efficacy and, ultimately, profits.

57. Upon information and belief, Defendant is compensated by third parties like Facebook, Google, and TikTok in the form of the use of the Pixel and similar technologies in exchange for disclosing the Private Information of its patients.

58. "Retargeting" is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

59. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiff and Class Members.

60. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

G. Cerebral Harmed Plaintiff and Class Members by Unlawfully Disclosing Their Private Information to Facebook, Google, TikTok, and Other Third Parties

64. Plaintiff Thomas entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Thomas disclosed her Private Information to Defendant.

65. Plaintiff Thomas accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's online solicitation.

[10] *See* 45 C.F.R. § 164.514(2); 45 C.F.R. § 164.514(2)(ii); 45 C.F.R. § 164.514(b)(2)(i)(O).

66. Plaintiff Thomas used Defendant's Website to research particular medical concerns and treatments, fill out forms and questionnaires, and perform other tasks related to her particular medical concerns.

67. In the course of using Defendant's services, Plaintiff provided her name, phone number, email address, date of birth, and other PII. As a result of the Tracking Pixel Defendant chose to install on its Website, this information was intercepted, viewed analyzed, and used by unauthorized third parties.

68. In the course of using Defendant's services, Plaintiff answered Defendant's online mental health self-assessment and communicated information regarding her particular health condition and concerns and other PHI. As a result of the Tracking Pixel Defendant chose to install on its Website, this PHI was intercepted, viewed analyzed, and used by unauthorized third parties.

69. Plaintiff Thomas reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

70. Plaintiff Thomas provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

71. As described herein, Defendant worked with Facebook, Google, TikTok, and others to intercept Plaintiff Thomas's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

72. By doing so without Plaintiff Thomas's consent, Defendant breached Plaintiff Thomas's right to privacy and unlawfully disclosed Plaintiff Thomas's Private Information to third parties.

73. Defendant did not inform Plaintiff Thomas that it had shared her Private Information with unauthorized third parties until on or around March 6, 2023.

74. Plaintiff Thomas and all similar situated Cerebral patients suffered damages in the form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

75. Plaintiff Thomas has a continuing interest in ensuring that her Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

V. CLASS ACTION ALLEGATIONS

76. Plaintiff brings this action individually and on behalf of all other persons similar situated, pursuant to Federal Rules of Civil Procedure 23 (b)(2), 23(b)(3), and 23(c)(4).

77. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website.**

78. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

79. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well add subclasses, before the Court determines whether certification is appropriate.

80. Numerosity, Fed. R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over 3,000,000 individuals whose Private Information may have been improperly accessed by Facebook, Google, and/or TikTok and the Class is identifiable within Defendant's records.

81. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to each Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant violated its Privacy Policies by disclosing the PII and PHI of Plaintiff and Class Members to Facebook, Google, TikTok, and/or additional third parties;
d. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI would be disclosed to third parties;
e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;
f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policies practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

82. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised as a result of Defendant's use of the Pixel and similar tracking technologies on its Website.

83. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind. Furthermore, Plaintiff has no conflicts of interest and seeks no relief that is antagonistic to those of the other Class Members.

84. Superiority, Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no

unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Cerebral. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

85. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

86. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is

representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

87. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

88. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

89. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to otherwise act unlawfully as set forth in this Complaint.

90. Further, Defendant has acted or refused to act on grounds generally applicable to each Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

91. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiff's and Class Members' Private Information with respect to Defendant's Privacy Policies;

c. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Class)

92. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

93. Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class, Defendant owed, and continue to owe, a duty to Plaintiff and

the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

94. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

95. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information through use of the Pixel and other tracking technologies would result in unauthorized third parties, such as Facebook, Google, and TikTok, gaining access to such Private Information for no lawful purpose.

96. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and common law. Defendant was in a position to ensure that the Website was designed in a way to protect against unauthorized disclosures, not enable them.

97. In addition, Defendant had a duty, under HIPAA privacy laws, to safeguard Plaintiff's and Class Members' Private Information from unauthorized disclosure. HIPAA was enacted with the objective of protecting the confidentiality of patient healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA not only applies to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

98. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Defendant's misconduct included the failure to (1) secure Plaintiff's and Class Members' Private

Information; (2) comply with HIPAA; (3) comply with industry standard data security practices; (4) implement adequate website and event monitoring; and (5) implement the systems, policies, and procedures necessary to prevent this type of unauthorized disclosure.

99. As a direct result of Defendant's breach of its duties owed to Plaintiff and Class Members, as set forth herein, and the resulting unauthorized disclosure of Plaintiff's and Class Members' Private Information to third parties such as Facebook, Google, and TikTok, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

100. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class Members' Private Information constituted (and continue to constitute) negligence at common law.

101. Plaintiff and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT II
BREACH OF CONTRACT
(On behalf of Plaintiff and the Class)

102. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

103. Plaintiff and Class Members entered into a valid and enforceable contract through which they entrusted their Private Information to Defendant in exchange for Defendant's healthcare services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

104. Cerebral's Privacy Policies memorialized the rights and obligations of Cerebral and its patients. This document states in relevant part: "By accessing or using the Services, you accept the practices and policies outlined in this Privacy Policy and you hereby consent that we may collect, use, and disclose your information as set forth in this Privacy Policy."

105. In the Privacy Policies, Cerebral expressly commits to protecting the privacy and security of Plaintiff's and Class Members' Private Information and promises to never share it except under certain limited circumstances.

106. Plaintiff and Class Members fully performed their obligations under their contracts with Cerebral.

107. However, Cerebral failed to secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Cerebral breached its contracts with Plaintiff and Class Members.

108. Specifically, through its admitted use of the Pixel and other tracking technologies, Cerebral allowed third parties such as Facebook, Google, and TikTok to access, copy, and/or use Plaintiff's and Class Members' Private Information without Plaintiff's and Class Members' knowledge or permission. Therefore, Cerebral breached the Privacy Policies with Plaintiff and Class Members.

109. Cerebral's failure to satisfy its confidentiality and privacy obligations, specifically those arising under its own Privacy Policies, HIPAA, and applicable industry standards, resulted in Cerebral providing services to Plaintiff and Class Members that were contrary to the agreement agreed upon by the parties.

110. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

111. As a direct and proximate result of Cerebral's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

112. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

113. This Count is pled in the alternative to Count II above.

114. Cerebral provides online mental healthcare services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members turning over their Private Information to Defendant in exchange for services.

115. Through its experience as an online healthcare provider, Cerebral knew or should have known that it needed to protect Plaintiff's and Class Members' confidential Private Information in accordance with its own Privacy Policies, business practices, and applicable law and industry standards.

116. As consideration, Plaintiff and Class Members turned over valuable Private Information to Cerebral. Accordingly, Plaintiff and Class Members bargained with Cerebral to securely maintain and store their Private Information.

117. Cerebral accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing online healthcare services to Plaintiff and Class Members.

118. In delivering their Private Information to Cerebral, Plaintiff and Class Members intended and understood that Cerebral would adequately safeguard the Private Information as part of its delivery of that service.

119. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to taking steps to ensure the confidentiality of the Private Information, and complying with HIPAA standards to make sure that Plaintiff's and Class Members' PHI would remain protected from unauthorized disclosure to third parties.

120. Plaintiff and Class Members would not have entrusted their Private Information to Cerebral in the absence of such an implied contract.

121. Had Cerebral disclosed to Plaintiff and the Class that they intended to utilize the Pixel to share their Private Information with third parties such as Facebook, Google, and TikTok rather than secure their sensitive data, Plaintiff and Class Members would not have provided their Private Information to Defendant.

122. As a provider of healthcare, Cerebral recognized (or should have recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and Class Members.

123. Cerebral violated these implied contracts by failing to employ reasonable and adequate measures to secure Plaintiff's and Class Members' Private Information to ensure that the Private Information was not shared with third parties without Plaintiff's and Class Members' consent. Cerebral further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

124. Additionally, Cerebral breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

125. Cerebral also breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or

software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

126. Cerebral further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

127. Cerebral further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

128. Cerebral further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI through its unauthorized use of the Pixel and other tracking technologies.

129. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Private Information to Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Private Information.

130. Plaintiff and Class Members have been damaged by Cerebral's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
INVASION OF PRIVACY
(On behalf of Plaintiff and the Class)

131. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

132. The highly sensitive and personal Private Information of Plaintiff and Class Members consists of private and confidential facts and information regarding

Plaintiff's and Class Members' mental health that were never intended to be shared beyond private communications on the Website and the consideration of health professionals.

133. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this Information against disclosure to unauthorized third parties, including Facebook, Google, TikTok, and others.

134. Defendant owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

135. Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information to Facebook, Google, and TikTok, third-party tech and marketing giants, is highly offensive to a reasonable person.

136. Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude and/or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

137. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiff's and Class Members' privacy because Defendant facilitated Facebook's, Google's, TikTok's, and others' unauthorized simultaneous eavesdropping and wiretapping of confidential communications.

138. Defendant failed to protect Plaintiff's and Class Members' Private Information and acted knowingly when it installed the Pixel onto the Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

139. Because Defendant intentionally and willfully incorporated the Pixel into the Website and encouraged individuals to use and interact with the Website

and the mental health screenings thereon, Defendant had notice and knew that its practices would cause injury to Plaintiff and the Class.

140. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information, including PII and PHI of Plaintiff and Class Members, was disclosed to at least three known unauthorized third parties, causing Plaintiff and the Class to suffer damages.

141. Plaintiff, on behalf of herself and Class Members, now seeks compensatory damages for Defendant's invasion of privacy, which damages include the value of the privacy interest invaded by Defendant, the loss of time and opportunity costs incurred by Plaintiff and Class Members, the lost benefit of the bargain Plaintiff and Class Members made with Defendant, plus pre-judgment interest and costs.

142. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendant and remains in the possession and control of Defendant, Facebook, Google, and TikTok.

143. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's and unauthorized third parties' continued possession of their sensitive and confidential Private Information. A judgment for monetary damages will not undo Defendant's disclosure of the Private Information to unauthorized third parties who, upon information and belief, continue to possess and utilize the Private Information.

COUNT V
BREACH OF CONFIDENCE
(On behalf of Plaintiff and the Class)

144. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

145. Possessors, such as Defendant, of non-public medical information have a duty to keep such medical information completely confidential.

146. Plaintiff and Class Members had reasonable expectations of privacy in the responses and communications entrusted to Defendant through the Website, which responses and communications included highly sensitive Private Information.

147. Contrary to its duties as a telehealth institution (and its express promises of confidentiality of the Private Information entrusted to it), Defendant installed the Pixel and other tracking technologies to disclose and transmit to third parties Plaintiff's and Class Members' Private Information, including data relating to Plaintiff's and Class Members' mental health.

148. These disclosures were made without Plaintiff's or Class Members' knowledge, consent, or authorization.

149. The third-party recipients included, but may not be limited to, Facebook, Google, and TikTok, as admitted by Defendant in its Notice to Plaintiff and the Class.

150. As a direct and proximate cause of Defendant's unauthorized disclosures of Plaintiff's and Class Members' Private Information, Plaintiff and Class Members were damaged by Defendant's breach of confidentiality in that (a) sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private; (b) Plaintiff and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements; (c) Defendant eroded the essential confidential nature of the mental health screenings that Plaintiff and Class Members participated in; (d) general damages for invasion of their rights in an amount to be determined by a jury at trial; (e) nominal damages for each independent violation; (f) the unauthorized use of something of value (the highly sensitive Private Information) that belonged to Plaintiff and Class Members and the obtaining of a benefit therefrom without Plaintiff's and Class members'

knowledge or informed consent and without compensation to Plaintiff or Class Members for the unauthorized use of such data; (g) diminishment of the value of Plaintiff's and Class Members' Private Information; and (h) violation of property rights Plaintiff and Class Members have in their Private Information.

COUNT VI
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

151. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

152. This count is pleaded in the alternative to Counts II and III above.

153. Defendant benefits from the use of Plaintiff's and Class Members' Private Information and unjustly retained those benefits at Plaintiff's and Class Members' expense.

154. Plaintiff and Class Members conferred a benefit upon Defendant in the form of the monetizable Private Information that Defendant collected from them and disclosed to third parties, including Facebook, Google, and TikTok, without authorization and proper compensation.

155. Defendant consciously collected and used this Information for their own gain, providing itself with economic, intangible, and other benefits, including substantial monetary compensation.

156. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff or Class Members.

157. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff or Class Members gratuitously and, thus, rightly belongs to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in Arizona and every other state for Defendant to be permitted to retain

any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, omissions, and trade practices alleged in this Complaint.

158. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT VII
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), 18 U.S.C. § 2511(1) *ET SEQ.* – UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On behalf of Plaintiff and the Class)

159. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

160. The ECPA protects both sent and received communications.

161. The ECPA, specifically 18 U.S.C. § 2520(a), provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

162. The transmissions of Plaintiff's and Class Members' Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition under 18 U.S.C. § 2510(12).

163. The transmission of Private Information between Plaintiff and Class Members and Defendant via the Website are "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

164. The ECPA defines "content" when used with respect to electronic communications to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

165. The ECPA defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

166. The ECPA defines "electronic, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;
b. Plaintiff's and Class Members' computing devices;
c. Defendant's web-servers; and
d. The Pixel deployed by Defendant to effectuate the sending and acquisition of user and patient sensitive communications.

167. By utilizing and embedding the Pixel on the Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

168. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to Facebook.

169. The intercepted communications included, but are not limited to, communications to and from Plaintiff and Class Members regarding PII and PHI, including name, Facebook ID, and mental health information relevant to the screenings in which Plaintiff and Class Members participated.

170. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to Facebook, Google, TikTok and, potentially, other third parties, while knowing or having reason to know that the Information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

171. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the Information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

172. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

173. Defendant intentionally used the wire or electronic communications to increase its profit margins. Specifically, Defendant used the Pixel and other tracking technologies to track and utilize Plaintiff's and Class Members' Private Information for financial support.

174. Defendant was not acting under color of law to intercept Plaintiff and Class Members' wire or electronic communications.

175. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy via the Pixel tracking code.

176. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

177. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Website, creation of accounts, and participation in Defendant's mental health screenings, Defendant's purpose was tortious and designed to violate federal and state law, including as described above, a knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person.

COUNT VIII
VIOLATIONS OF THE ECPA, 18 U.S.C. § 2511(3)(A) – UNAUTHORIZED DIVULGENCE
(On behalf of Plaintiff and the Class)

178. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

179. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

180. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

181. Defendant's Website is an electronic communication service in that it gives patients the ability to send electronic communications to Defendant as responses to Defendant's mental health screenings and assessments. In the absence of Defendant's Website, internet users could not have submitted such

communications in creating their accounts and participating in mental health screenings.

182. Defendant's Website is a conduit of communication between Plaintiff and Class Members and Defendant (and Defendant's health professionals).

183. Defendant intentionally designed and/or implemented the Pixel and other tracking technologies and was or should have been aware that such tools could divulge Plaintiff's and Class Members' Private Information to unauthorized parties.

184. Upon information and belief, Defendant's divulgence of the contents of Plaintiff's and Class Members' confidential communications was contemporaneous with their exchange with Defendant's Website, to which they directed their communications.

185. Defendant divulged the contents of Plaintiff's and Class Members' electronic communications without authorization.

186. Defendant divulged the contents of Plaintiff's and Class Members' communications to Facebook, Google, TikTok, and others without Plaintiff's and Class Members' consent and/or authorization.

187. Exceptions do not apply. In addition to the exception for communications directly to Defendant or an agent of Defendant, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication":

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title";
b. "with the lawful consent of the originator or any addressee or intended recipient of such communication";
c. "to a person employed or authorized, or whose facilities are used, to forward such communications to its destination"; or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency." *See* U.S.C. § 2511(3)(b).

188. Section 2511(2)(1)(i) also provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

189. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on the Website to Facebook, Google, TikTok, and other third parties was not authorized by y 18 U.S.C. § 2511(2)(a)(i) in that it was neither (a) a necessary incident to the rendition of Defendant's service; nor (b) necessary to the protection of the rights or property of Defendant.

190. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

191. Defendant's divulgence of the contents of participant communications on Defendant's browser through the Pixel's code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above, (a) Plaintiff and Class Members did not authorize Defendant to divulge the contents of their communications; and (b)

Defendant did not procure the "lawful consent" from the Website through which Plaintiff and Class Members were exchanging their Private Information.

192. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

193. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

194. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT IX
VIOLATIONS OF TITLE II OF THE ECPA, 18 U.S.C. § 2702, *ET SEQ.* – STORED COMMUNICATIONS ACT
(On behalf of Plaintiff and the Class)

195. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

196. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

197. The ECPA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

198. Defendant's Website is a conduit of communication between Plaintiff and Class Members and Defendant (and Defendant's health professionals), and Defendant's business is based, in large part, on the provision of electronic communications. Indeed, it is a telecommunications healthcare business.

199. Defendant intentionally procures and embeds various Private Information belonging to Plaintiff and Class Members through the Pixel and other tracking technologies used on the Website, thus further qualifying as an electronic communication service.

200. The ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

201. Defendant stores the content of Plaintiff's and Class Members' communications with the Website and files associated with it using the Pixel and/or other tracking technologies. Through these tracking technologies, Defendant is able to store Plaintiff's and Class Members' Private Information on its servers and then transmit that Private Information to Facebook, Google, TikTok, and other third parties.

202. When Plaintiff and/or Class Members communicate with the Website via account creation and participation in Defendant's mental health screenings, the content of such communications is immediately placed into storage.

203. Defendant knowingly divulges the contents of these stored communications through the Website's source code.

204. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a communication":

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient";

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title";

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service";

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination";

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service";

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A";

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime";

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

205. 183. Defendant did not divulge the contents of Plaintiff's and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiff and Class Members.

206. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

207. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

208. Defendant's divulgence of the contents of Plaintiff's and Class Members' communications on the Website to Facebook, Google, TikTok, and others was not authorized by 18 U.S.C. 2511(2)(a)(i) in that such divulgence was neither (a) a necessary incident to the rendition of Defendant's services; nor (b) necessary to the protection of the rights or property of Defendant.

209. Defendant's divulgence of the contents of its patients' communications on the Website was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above, (a) neither Plaintiff nor Class Members authorized Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Website through which Plaintiff and Class Members were exchanging their Private Information.

210. Moreover, Defendant divulged the contents of Plaintiff's and Class Members' communications through the Pixel to individuals who are not "person[s]

employed or whose facilities are used to forward such communication to its destination."

211. The contents of Plaintiff's and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

212. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages, if applicable, in an amount to be determined by a jury at trial; and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT X
VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT ("CFAA"), 18 U.S.C. § 1030, *ET SEQ.*
(On behalf of Plaintiff and the Class)

213. Plaintiff restates and realleges all of the allegations stated in paragraphs 1 through 91 as if fully set forth herein.

214. Plaintiff's and Class Members' computers and/or mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

215. Defendant exceeded, and continues to exceed, its authorized access by gaining access to Plaintiff's and Class Members' protected computers and other electronic devices and obtaining information thereby, in violation of 18 U.S.C. §§ 1030(a)(2), 1030(a)(2)(C).

216. For example, Defendant accessed Plaintiff's and Class Members' Private Information under false pretenses, *i.e.*, by failing to disclose that they were

transmitting the Private Information to Facebook, Google, TikTok, and other third parties.

217. Moreover, Defendant exceeded its unauthorized access in violation of its own Privacy Policies by disclosing Plaintiff's and Class Members' Private Information to Facebook, Google, TikTok, and other third parties.

218. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), inter alia, due to the secret transmission of Plaintiff's and Class Members' Private Information – including their communications and interactions with the Website, URLs of webpages visited, and/or other electronic communications in real-time, which were never intended for disclosure and public consumption.

219. Defendant's conduct also constitutes a "threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the sensitive nature of the Private Information of Plaintiff and the Class being made available, by Defendant, to Facebook, Google, TikTok, and/or other third parties without adequate privacy protections.

220. Accordingly, Plaintiff and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." *See* 18 U.S.C. § 1030(g).

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, respectfully requests this Court enter an Order:

a. Certifying this case as a class action on behalf of the Nationwide Class defined above, appointing Plaintiff as representative of the Class, and appointing her counsel as Class Counsel;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or unauthorized disclosure of Plaintiff's and Class Members' Private Information;

c. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

d. For an award of damages, including but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f. Pre- and post-judgment interest on any amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: April 24, 2023

Respectfully submitted,

/s/ Kyle McLean

Kyle McLean, SBN #330580
Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
700 S. Flower Street, Ste. 1000
Los Angeles, CA 90017
Telephone: 213-376-3739
E: kmclean@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

**Pro hac vice applications forthcoming*

Attorneys for Plaintiff and the Class